

AP PHOTO. JERRY HOEFER



FBI SPECIAL Agent Michael Morris, right, compares notes with Paul Coggins, U.S. attorney for the North District of Texas, at the North Texas Regional Computer Forensics Laboratory in Dallas. At the time (August 2000), it was only one of two such cybercrime-fighting labs.

FBI Fights the Bandwidth Brigands

The latest chapter in the history of extortion now means doing battle with evil “Bots.” In the 21st century, they come with ransom demands attached.

Editor's note: Earlier this year Mark Greisiger spoke with Thomas X. Grasso Jr., supervisory special agent of the Federal Bureau of Investigation's National Cyber-Forensics and Training Alliance. Grasso highlighted the ease with which villains of cyberspace can paralyze a network and make off with a hefty bundle of cash. An edited version of the conversation follows.

Mark Greisiger: Do you think cyberextortion is something businesses should be concerned about and take seriously?

Thomas X. Grasso Jr.: Absolutely, they should be concerned, especially if they have a Web-centric business model and depend on their network servers and availability of same for making their revenue.

MG: Any thoughts as to how frequent these events occur to date?

TG: FBI doesn't have formal statistics yet which breakout cyberextortion, but the scope of the problem—based on conversations with other agents, businesses—is that it is something that happens on a daily basis.

MG: What type of company might be targeted?

TG: Somebody whose business depends on their online presence, but also a company that is not so big that they have a distributed network or other best practices in place. This might be a business that operates on a small-to-medium size IT and security budget. They might be a target because they don't have the bandwidth in place or solutions like Akamai to mitigate a massive DDoS (distributed denial of service) attacks. Often we will see the bad guys doing some reconnaissance ahead of time on their targeted servers. They may even try a “test DoS” to see how the targeted servers respond to only a “slow down” scenario, before considering whether they're an ideal target. Of course, there are also businesses that operate offshore that might offer, for example, online gambling. These are a favorite target.

MG: Should a company pay a cyberextortion demand, especially under a scenario in which they know the attack capability of the bad guy is real?

TG: My opinion is that a company being extorted should not pay, but having said that, we realize that some probably do. I don't think

“NETDILIGENCE HAS PERSONALLY SEEN \$25,000 DEMANDS FROM COMPANIES THAT WE ASSESS ON BEHALF OF THEIR NETWORK INSURER.”

—Mark Greisiger, president,
NetDiligence

anyone should pay. Ethical reasons aside, the perpetrator is going to come back again and again. Giving in once leads often to repeat demands. You'll possibly end up making payments on a regular basis. Instead, a company might want to just bite the bullet and spend it on some form of mitigation.

MG: What might be the typical monetary amount often sought by bad guy? NetDiligence has personally seen \$25,000 demands from companies that we assess on behalf of their network insurer.

TG: I've heard numbers all over the place, though, so can't really say a given average.

MG: For companies or their insurers under a policy that pay the extortion, can you comment on catching the bad guy and the possibility of recovering any extorted funds?

TG: Regardless of where the subject is, if we catch him and get a conviction, restitution can be a remedy. It depends on the situation, but there are mechanisms in our current crime laws that permit restitution. Also, I'd say that we are getting more cooperation now than we have ever had from our counterparts overseas where we

didn't get maybe 10 years ago. So, we have a much better chance of a successful prosecution on an international case.

MG: Where do these attacks often originate from?

TG: I would rather not comment.

MG: Why do these DDoS attacks

appear to be often successful? What network security safeguard controls are lacking?

TG: The nature of DDoS has dramatically changed over the last five years due to the prevalence of high bandwidth Internet connections such as DSL and cable. \$45 a month gets a lot of cheap bandwidth which can place a user

on equal footing with businesses that use a T1. We are also seeing much more malicious software aimed at turning personal computers into 'Bots.' For example, we might witness an attack with 70,000 to 100,000 computers that are under the control of a single bad guy. With all these personal computers each having high bandwidth, you're wielding a powerful weapon against a single target, especially the business owner without redundant network access.

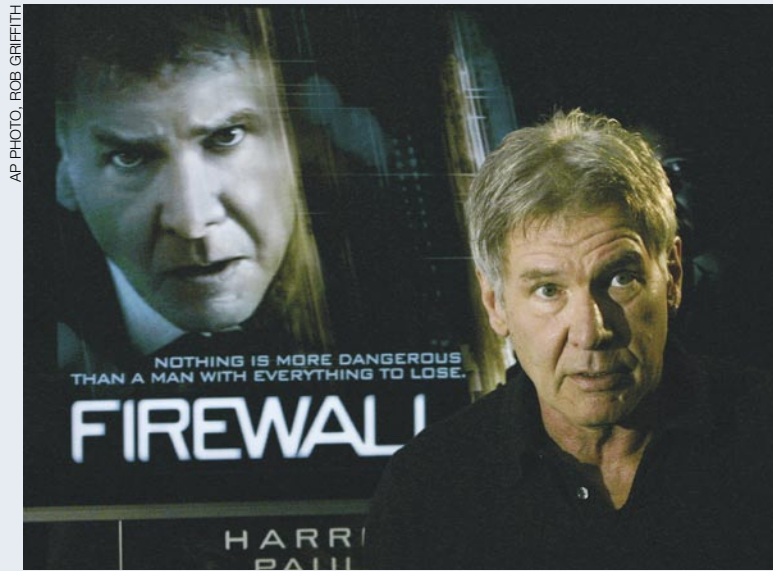
MG: What might a company do proactively to mitigate this exposure?

TG: First and foremost, they should have an incident response plan. They need to take the time to think about how they're going to react, so that you're not panicking when the real thing occurs. They should also contact law enforcement prior to event and make sure contacts are known. Establish a relationship with the special agents who investigate cybercrime matters in your area.

MG: Is there anything a business can do to make the FBI's efforts more effective?

TG: Yes, computer server logs can help in the investigation of the matter. The more logging the better. Network administrators and chief security officers should ensure that traffic is being logged at perimeters, as well as inside their network.

MARK GREISIGER is the president of NetDiligence. He can be reached at riskletters@lrp.com.



Network Extortion That's No Fiction

In the recent movie "Firewall," Harrison Ford's character, a banking security expert, is the victim of identity theft by perpetrators who attempt to force his assistance in a \$100 million robbery. While amusing to mass audiences, the storyline begs the question: fact or fiction?

From pervasive global outbreaks to smaller, stealthier attacks targeted at specific organizations for extortion purposes, a fundamental shift, or evolution, in cybercrime is anticipated in 2006, according to the IBM Global Business Security Index Report.

High-profile arrests in the United States and around the world indicate criminal gangs are increasingly using the Internet as a tool to extort money from businesses.

The cost of a distributed denial of service attack can be substantial—anywhere from \$300

to \$13 million per person per incident—and it has been estimated that as many as 10,000 incidents occur worldwide each day.

In fact, according to the SANS Institute, a computer security training, certification and research organization, the FBI receives more than one report of cyberextortion every day.

From ransomware, malicious software that encrypts computer files and asks for a ransom to decrypt them, to the cyberextortionists who demand huge sums of money to cease their attacks, the financial impact can vary.

Chief information officers see this crime as a greater threat than physical crime, according to a recent IBM survey of manufacturing, financial, health-care and retail enterprises. Businesses that are victims of such extortion may suffer a loss of customer and shareholder confidence, reduced productivity and a massive dip in revenue.

Intended victims may look to properly drafted insurance, such as a network-risk policy to cover loss arising from extortion threats regarding computer networks and intangible assets. Property policies, as well as kidnap and ransom policies, can also cover business interruption and extra expenses.

Now, if only Hollywood would open its eyes to the appeal of insurance as one of the big-screen heroes, instead of giving Harrison Ford all of the fun.

—Kevin Kalinich is co-national managing director of professional risk solutions for Aon Financial Services Group. He can be reached at www.riskletters@lrp.com.